CERTIFICATION

I, Kohno Takao; 4-3 Tsurigane-cho, 2-chome, Chuo-ku, Osaka 540-0035 JAPAN, hereby certify that each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.

KOHNO Takao

Dated this 15th **day of** May, 2009

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-047946
(43)Date of publication of application : 18.02.2000

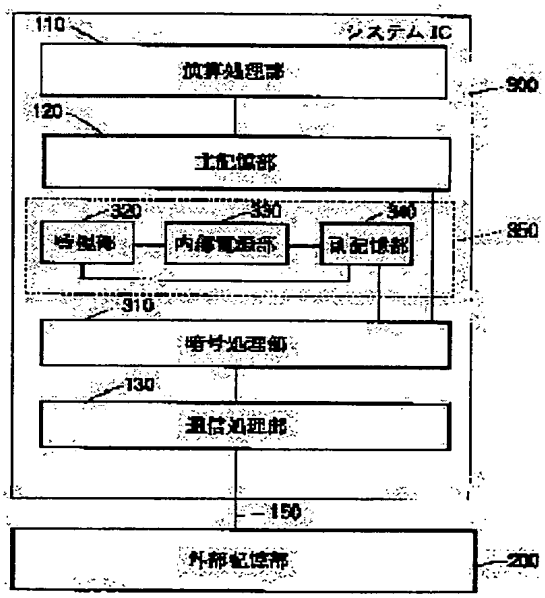
(51)Int.Cl. G06F 12/14

(21)Application number : 10-212357
(22)Date of filing : 28.07.1998

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : JINNAI HIDETO
FUJII TAMOTSU

(54) INTEGRATED CIRCUIT DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an integrated circuit device capable of keeping the safety of a system from the threat of illegal use by analyzing/falsifying a program or data.
SOLUTION: A code processing part 310 for decoding the program or data from an external storage part 200 and encoding the data when writing the data into the external storage part 200, a monitoring part 320 for monitoring access from the outside to a system IC 300, an internal power source part 330 having a function for supplying power to a sub storage part 340 and monitoring part 320 and cutting the supply of power to a sub storage part 340 when there is a power supply cutting indication from the monitoring part 320, and the sub storage part 340 for holding an encoding/decoding key based on the supply of power from the internal power source part 330 are integrated in the system IC 300 and these components are made into one chip.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－47946
（P2000－47946A）
(43)公開日　平成12年２月18日(2000.2.18)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｄ　５Ｂ０１７

審査請求　未請求　請求項の数６　ＯＬ　（全８頁）

(21)出願番号　特願平10－212357

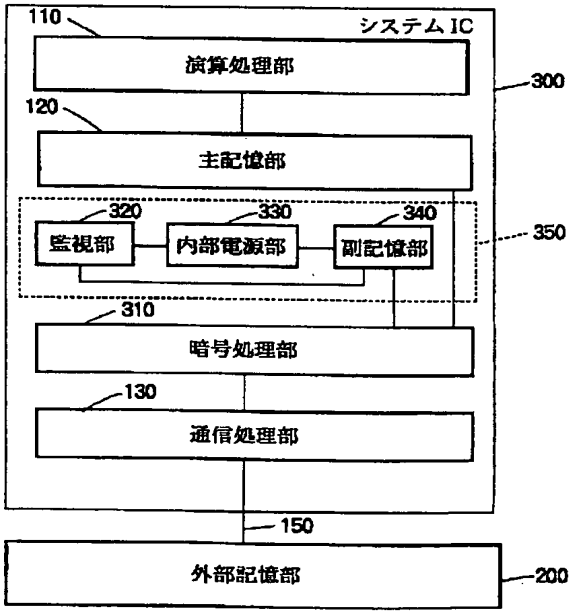
(22)出願日　平成10年７月28日(1998.7.28)

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号
(72)発明者　陣内　秀人
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内
(72)発明者　藤井　保
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内
(74)代理人　100083840
弁理士　前田　実

Ｆターム(参考)　5B017 AA01 AA07 BA07 BA08 BB03 CA13 CA14

(54)【発明の名称】　集積回路装置

(57)【要約】
【課題】　プログラムやデータの解析・改竄による不正な使用の脅威からシステムの安全を保持することのできる集積回路装置を提供する。
【解決手段】　システムＩＣ３００は、外部記憶部２００からのプログラムやデータを復号化するとともに、外部記憶部２００にデータを書き出す時にデータの暗号化を行う暗号処理部３１０と、システムＩＣ３００に対する外部からのアクセスを監視する監視部３２０と、副記憶部３４０及び監視部３２０に電源を供給し、監視部３２０から電源遮断指示があると副記憶部３４０への電源供給を遮断する機能を有する内部電源部３３０と、内部電源部３３０の電源供給により暗号化鍵／復号化鍵を保持する副記憶部３４０とを組込み、かつこれらを１チップ化して構成する。



システムICの構成図

1

【特許請求の範囲】
【請求項１】　演算処理部、主記憶部、通信制御を行う通信処理部を備え、外部記憶装置とアクセス可能な集積回路装置において、
前記外部記憶装置からのプログラム及びデータを復号化するとともに、前記外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、
内部電源部の電源供給により暗号化鍵／復号化鍵を保持する副記憶部と、
集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると電源遮断指示する監視部と、
前記副記憶部に電源を供給し、前記監視部から電源遮断指示があると前記副記憶部への電源供給を遮断する機能を有する内部電源部とを備えたことを特徴とする集積回路装置。
【請求項２】　演算処理部、主記憶部、通信制御を行う通信処理部を備え、外部記憶装置とアクセス可能な集積回路装置において、
前記外部記憶装置からのプログラム及びデータを復号化するとともに、前記外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、
暗号化鍵／復号化鍵を保持する副記憶部と、
集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると前記副記憶部の記憶内容を書き換える監視部とを備えたことを特徴とする集積回路装置。
【請求項３】　前記不正アクセスは、
集積回路装置に対して外部からの読み出し／書き込みが通常と異なるアクセスであることを特徴とする請求項１又は２の何れかに記載の集積回路装置。
【請求項４】　前記不正アクセスは、
集積回路装置に設置された不正検知センサによる検知信号の入力であることを特徴とする請求項１又は２の何れかに記載の集積回路装置。
【請求項５】　請求項１記載の集積回路装置において、
前記暗号処理部、前記副記憶部、前記監視部及び前記内部電源部は、
集積回路装置内に組込み１チップ化して構成されたことを特徴とする集積回路装置。
【請求項６】　請求項１、２、３、４又は５の何れかに記載の集積回路装置において、
集積回路装置は、電子マネーシステムの電子マネーの決済部に用いられるＩＣであることを特徴とする集積回路装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、集積回路装置に係り、特に、電子マネーシステムの電子マネーの決済部に用いられる集積回路装置に関する。
【０００２】

2

【従来の技術】エレクトロニック・コマース（Electronic Commerce:電子商取引）では、現金通貨が有する決済機能（買手から売手へ経済価値を移転する機能）を、電子マネーという電子的な通貨情報（以下、電子マネー情報という。）で代替している。
【０００３】一般に、電子マネーを決済手段として機能させるためには、銀行等の金融機関を介在させないで、電子マネーを流通させるＩＣカード型の電子マネーシステム、あるいは銀行による決済を取引に介在させ、電子マネー情報をオンラインで決済するネットワーク型の電子マネーシステムのいずれかが構築されていなければならない。前者の電子マネーシステムでは、ＩＣカードにディジタルデータとして電子マネー情報を記録して、それを通貨情報として書き換えていくことができる。この電子マネーシステムで使用されるマネーカードは、通信機能、携帯機能、計算機能、及び管理機能等、種々の機能を有する。この結果、現金通貨に比較すると、電子マネー情報を記録したＩＣカードは、その情報をネットワークを介して遠隔地に瞬時に送れる、電子財布に入れておけば、かさばらずに携帯できる、売上の計算が簡単にできる、いつ、いくら使ったか等の記録がとれる等のメリットがある。
【０００４】今日、実験的に運用されているＩＣカード型の電子マネーカードシステムは、データの偽造や改竄等の脅威から、個別の金融機関の決済機構と連動されている。したがって、金融機関と利用者との間の資金の移動や、利用者相互間における資金の移動のためにＩＣカード（電子マネーカード）を発行し、また、電子マネーカードへの電子マネーの出金、電子マネーカードから電子マネーの入金、各口座間での振替処理等を管理するために、マネー管理センタが必要とされている。また、後者のネットワーク型の例としては、銀行間等のネットワークによる電子決済があり、セキュリティを確保するために専用回線を介して運用されている。
【０００５】また、電子マネーの発行機関と契約を行った加盟店は、簡易決済端末が設置され、店頭での小口決済が可能となる。すなわち、加盟店は買物代金の決済時に、簡易決済端末に利用者のＩＣカードを挿入し、売り上げ金額を入力することにより簡易決済端末の内蔵ＩＣカードへ該当金額の価値を移して決済を行う。このように、利用者ＩＣカードから端末内ＩＣカードへの電子マネーの移転、または利用者ＩＣカードからワレット（電子財布）内ＩＣカードに集金された電子マネーの端末内ＩＣカードへの移転を実現する。
【０００６】電子マネーの決済端末としては、例えば図５に示すものがある。
【０００７】図５は電子マネーの決済部として用いられる従来のシステムＩＣ（集積回路装置）の構成を示す図である。
【０００８】図５において、１００は決済端末内部に設

けられＩＣカードにアクセス可能なシステムＩＣ、２００はシステムＩＣ１００の外部に設置されシステムＩＣ１００にデータを供給するＲＡＭ，ＲＯＭ等の外部記憶部、１５０はシステムＩＣ１００と外部記憶部２００とを接続する信号線である。

【０００９】システムＩＣ１００は、ＣＰＵ等からなる演算処理部１１０と、高速動作可能なキャッシュメモリ等からなる主記憶部１２０と、バス制御及び外部との通信制御を行う通信処理部１３０とから構成される。また、システムＩＣ１００を動作させるプログラムやシステムＩＣ１００で処理するデータはシステムＩＣ１００の中にはない外部記憶部２００に格納している。

【００１０】システムＩＣ１００は、外部記憶部２００から一度取り寄せたデータを主記憶部１２０に記憶し、次回からの読み出しの際は、主記憶部１２０にキャッシュされた情報を読み出すことでデータを再度取り寄せなくてもよいようにするキャッシュ機能を有する。

【００１１】以上の構成において、システムＩＣ１００は、立ち上げ時に通信処理部１３０が外部記憶部２００から信号線１５０上を通してプログラムを主記憶部１２０に読み込み、演算処理部１１０は主記憶部１２０のプログラムによって動作を開始する。処理するデータは外部記憶部２００から通信処理部１３０を経由してプログラムを主記憶部１２０に読み込み、演算処理部１１０は主記憶部１２０のデータをプログラムにより指定された方法でデータ処理した後、外部記憶部２００に書き込む。

【００１２】

【発明が解決しようとする課題】しかしながら、このような従来のシステムＩＣにあっては、以下のような問題点があった。

【００１３】すなわち、従来のシステムＩＣでは、動作するプログラムをシステム上でなく外部記憶部２００上に記憶しているため、第三者に外部記憶部２００からプログラムを読み出されたり、外部記憶部２００とシステムＩＣ間の信号線１５０上を通信するプログラムを読み取られることでプログラムを解析・改竄されシステムを不当に使用される危険がある。

【００１４】また、データについても外部記憶部２００に記憶しているため、外部記憶部２００からデータを読み出されたり、外部記憶部２００とシステムＩＣ間の信号線１５０上を通信するデータを読み取られることでデータを改竄され不正なデータ処理に使用される危険がある。

【００１５】本発明は、プログラムやデータの解析・改竄による不正な使用の脅威からシステムの安全を保持することのできる集積回路装置を提供することを目的とする。

【００１６】

【課題を解決するための手段】本発明に係る集積回路装置は、演算処理部、主記憶部、通信制御を行う通信処理部を備え、外部記憶装置とアクセス可能な集積回路装置において、外部記憶装置からのプログラム及びデータを復号化するとともに、外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、内部電源部の電源供給により暗号化鍵／復号化鍵を保持する副記憶部と、集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると電源遮断指示する監視部と、副記憶部に電源を供給し、監視部から電源遮断指示があると副記憶部への電源供給を遮断する機能を有する内部電源部とを備えて構成する。

【００１７】本発明に係る集積回路装置は、演算処理部、主記憶部、通信制御を行う通信処理部を備え、外部記憶装置とアクセス可能な集積回路装置において、外部記憶装置からのプログラム及びデータを復号化するとともに、外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、暗号化鍵／復号化鍵を保持する副記憶部と、集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると副記憶部の記憶内容を書き換える監視部とを備えて構成する。

【００１８】上記不正アクセスは、集積回路装置に対して外部からの読み出し／書き込みが通常と異なるアクセスであってもよく、また、上記不正アクセスは、集積回路装置に設置された不正検知センサによる検知信号の入力であってもよい。

【００１９】本発明に係る集積回路装置は、暗号処理部、副記憶部、監視部及び内部電源部が、集積回路装置内に組込み１チップ化して構成されたものであってもよく、また、本発明に係る集積回路装置は、電子マネーシステムの電子マネーの決済部に用いられるＩＣであってもよい。

【００２０】

【発明の実施の形態】本発明に係る集積回路装置は、電子マネーシステムの電子マネーの決済部に用いられるシステムＩＣに適用することができる。

【００２１】第１の実施形態

図１は本発明の第１の実施形態に係る集積回路装置の構成を示すブロック図である。本実施形態に係る集積回路装置の説明にあたり前記図５と同一構成部分には同一符号を付している。

【００２２】図１において、３００は決済端末内部に設けられＩＣカードにアクセス可能なシステムＩＣ（集積回路装置）、２００はシステムＩＣ３００の外部に設置されシステムＩＣ３００にデータを供給するＲＡＭ，ＲＯＭ等の外部記憶部（外部記憶装置）、１５０はシステムＩＣ３００と外部記憶部２００とを接続する信号線である。

【００２３】システムＩＣ３００は、ＣＰＵ等からなる演算処理部１１０と、高速動作可能なキャッシュメモリ等からなる主記憶部１２０と、バス制御及び外部との通

信制御を行う通信処理部１３０と、外部記憶部２００からのプログラムやデータを復号化するとともに、外部記憶部２００にデータを書き出す時にデータの暗号化を行う暗号処理部３１０と、システムＩＣ３００に対する外部からのアクセスを監視する監視部３２０と、副記憶部３４０及び監視部３２０に電源を供給し、監視部３２０から電源遮断指示があると副記憶部３４０への電源供給を遮断する機能を有する内部電源部３３０と、内部電源部３３０の電源供給により記憶内容（暗号化鍵／復号化鍵）を保持する副記憶部３４０とから構成される。

【００２４】システムＩＣ３００を動作させるプログラムやシステムＩＣ３００で処理するデータは、暗号化されたデータとして外部記憶部２００に保管されている。また、システムＩＣ３００は、外部記憶部２００から一度取り寄せた暗号化データを、復号化して主記憶部１２０に記憶し、次回からの読み出しの際は、主記憶部１２０にキャッシュされた情報を読み出すことでデータを再度取り寄せなくてもよいようにするキャッシュ機能を有する。

【００２５】システムＩＣ３００と外部記憶部２００の間は従来例と同様に信号線１５０により接続されているが、信号線１５０上を経由するプログラムや処理データは全て暗号化されている。

【００２６】上記監視部３２０、内部電源部３３０及び副記憶部３４０は、全体として監視手段３５０を構成する。

【００２７】図２は上記監視手段３５０の構成を詳細に示すブロック図である。

【００２８】図１及び図２において、暗号処理部３１０は、外部記憶部２００のプログラムを読み込む場合やデータを読み込む時に復号化し、外部記憶部２００にデータを書き出す時にデータの暗号化を行う。暗号化／復号化に使用する暗号化鍵／復号化鍵は、監視手段３５０の副記憶部３４０に記憶されている。

【００２９】副記憶部３４０は、暗号化／復号化に使用する暗号化鍵／復号化鍵として、公開鍵暗号方式であるＲＳＡ方式と秘密鍵方式であるＤＥＳ（Data Encryption Standard），ＦＥＡＬ等を併用する。例えば、暗号化鍵として、例えば６４bitのＤＥＳを用いるとともに、暗号処理の基本方式としてプログラム、データ、その他の部分の暗号処理は、異なる方式をとる。また、暗号処理は、副記憶部３４０の暗号化鍵／復号化鍵を使用した暗号処理部１３０が、システムＩＣ３００内において行う。

【００３０】監視部３２０は、マイクロプロセッサ等により構成され、システムＩＣ３００に対する外部からのアクセスを常に監視し、システムＩＣ３００に対して不正なアクセスがあった時、内部電源部３３０に電源遮断指示を出して副記憶部３４０への電源供給を遮断させ、副記憶部３４の暗号化鍵／復号化鍵を消去する。

【００３１】ここで、上記不正なアクセスには、システムＩＣ３００に対して外部からの読み出し／書き込みが通常と異なるアクセスを判別した場合と、システムＩＣ３００に設置されたセンサから不正アクセス信号が入力された場合とがある。前者、すなわちシステムＩＣ３００に対する外部からの読み出し／書き込みが通常と異なるアクセスである場合には、システムＩＣ３００に対して外部からプログラムやデータの解析・改竄のためのアクセスが行われた可能性があると判断して内部電源部３３０に電源遮断指示を出力する。

【００３２】また、システムＩＣ３００、特に監視手段３５０を収容する筐体には、該筐体内部を開けたり衝撃を感知したときに応答するセンサが設置されており、センサ出力は監視部３２０に入力されている。上記後者は、このセンサから不正アクセス信号が入力された場合であり、このセンサ入力があった場合には、システムＩＣ３００を外部から物理的にアクセス（破壊）してプログラムやデータの解析・改竄を行う場合であると判断して内部電源部３３０に電源遮断指示を出力する。

【００３３】内部電源部３３０は、副記憶部３４０及び監視部３２０に電源を供給し、監視部３２０から電源遮断指示があると副記憶部３４０への電源供給を遮断する。

【００３４】副記憶部３４０は、暗号化／復号化に使用する暗号化鍵／復号化鍵を記憶するもので、内部電源部３３０の電源供給により内容を保持する半導体メモリ（例えば、ＤＲＡＭ）からなる。副記憶部３４０は、内部電源部３３０からの電源供給が絶たれると、極めて短い時間に記憶内容が消失する。

【００３５】本実施形態に係るシステムＩＣ３００は、システムＩＣ３００内に暗号処理部３１０、監視部３２０、内部電源部３３０及び副記憶部３４０を組込み、かつこれらが１チップ化されて構成されている。したがって、これら回路部を単独で取り出すことは極めて困難であるとともに、暗号化鍵／復号化鍵を記憶する副記憶部３４０は内部電源部３３０によりバックアップされ、監視部３２０が不正アクセスを検知すると前記バックアップを遮断して副記憶部３４０の内容を消去する。

【００３６】以下、上述のように構成されたシステムＩＣ３００の動作を説明する。

【００３７】〔全体動作〕システムＩＣ３００は、立ち上げ時の動作は通信処理部１３０がプログラムを外部記憶部２００から暗号化された状態で読み込む。読み込まれたプログラムは、副記憶部３４０に記憶されている復号化鍵を使用して暗号処理部１３０で復号化され、主記憶部１２０に書き込まれる。演算処理部１１０は、主記憶部１２０からプログラムを読み込み、プログラムを実行する。

【００３８】システムＩＣ３００で処理するデータは、外部記憶部２００に暗号化された状態で記憶されてい

る。システムＩＣ３００がデータを読み込む場合は、まず通信処理部１３０が通信線１５０を通して外部記憶部２００からデータを読み込み、読み込んだデータを暗号処理部３１０が副記憶部３４０に記憶されている復号化鍵を使用して復号化する。復号化したデータは主記憶部１２０に書き込まれる。

【００３９】演算処理部１１０は、主記憶部１２０に格納されたプログラムによりデータを処理する。

【００４０】演算処理部１１０で処理されたデータは暗号処理部３１０に出力され、暗号処理部３１０が副記憶部３４０に記憶された暗号化鍵を使用して暗号化する。暗号化したデータは、通信処理部１３０により通信線１５０を通して外部記憶部２００に書き出される。

【００４１】〔監視部３２０の監視動作〕システムＩＣ３００は、未使用時も内部電源部３３０によりバックアップされ、監視部３２０が外部からのアクセスを監視している。監視部３２０の監視により、システムＩＣ３００に対して外部から通常と異なったアクセス（不正アクセス）があった場合には、監視部３３０は、内部電源部３３０に電源遮断指示を出して副記憶部３４０への電源供給を遮断させ、副記憶部３４の暗号化鍵／復号化鍵を強制的に消去する。これにより、鍵の盗難を防止する。上記不正アクセスには、前述したように通常と異なる手順や不当なアドレス指定によるアクセスの他、システムＩＣ３００に設置されたセンサからの入力がある。

【００４２】また、内部電源部３３０から供給される電圧が所定値以下となったときも安全性を確保するため、監視部３３０が、内部電源部３３０に電源遮断指示を出して副記憶部３４０への電源供給を遮断させ、副記憶部３４のデータを消去する。すなわち、内部電源部３３０は規定の使用期間及び通常の使用状態・方法の範囲では、一定電圧を出力するように構成されており、この出力電圧が所定値以下となったときは内部電源部３３０自身が消耗した時を含め安全性の確保が図れなくなった状態であるので、監視部３３０が副記憶部３４のデータを消去する。

【００４３】図３は監視手段３５０の監視部３２０の監視動作を示すフローチャートであり、監視部３２０のプロセッサにより所定タイミングで繰り返し実行される。図中、ＳＴはフローの各ステップを示す。

【００４４】ステップＳＴ１に示される状態は、システムＩＣ３００のイベント待ち状態である。このイベント待ち状態において、内部電源部３３０の出力電圧のチェックを行い、内部電源部３３０の出力電圧が所定値より大きければ内部電源部３３０について異常はないと判断してステップＳＴ２に進み、出力電圧が所定値以下のときは内部電源部３３０に異常があると判断してステップＳＴ５に進む。

【００４５】ステップＳＴ２では、システムＩＣ３００に対する外部からのデータをチェックし、システムＩＣ３００に対して外部からの読み出し／書き込みに不正アクセスがないときはステップＳＴ３でセンサ入力が正常か否かを判別する。

【００４６】センサ入力が正常であるときは不正使用がないと判断してステップＳＴ４で該当処理を行ってステップＳＴ１に戻り上記処理を繰り返す。

【００４７】一方、上記ステップＳＴ１で内部電源部３３０の出力電圧が所定値以下のとき、上記ステップＳＴ２で不正アクセスがあったとき、あるいは上記ステップＳＴ３でセンサ入力に異常があったときは、システムＩＣ３００に対して外部からプログラムやデータの解析・改竄のための不正使用が行われたと判断して内部電源部３３０に電源遮断を指示し、内部電源部３３０から副記憶部３４０への電源供給を遮断する。これにより、副記憶部３４内の暗号化鍵／復号化鍵を消去する。

【００４８】以上説明したように、第１の実施形態に係るシステムＩＣ３００は、外部記憶部２００からのプログラムやデータを復号化するとともに、外部記憶部２００にデータを書き出す時にデータの暗号化を行う暗号処理部３１０と、システムＩＣ３００に対する外部からのアクセスを監視する監視部３２０と、副記憶部３４０及び監視部３２０に電源を供給し、監視部３２０から電源遮断指示があると副記憶部３４０への電源供給を遮断する機能を有する内部電源部３３０と、内部電源部３３０の電源供給により暗号化鍵／復号化鍵を保持する副記憶部３４０とを組込み、かつこれらを１チップ化して構成し、暗号化鍵／復号化鍵を記憶する副記憶部３４０は内部電源部３３０によりバックアップされ、監視部３２０が不正アクセスを検知するとバックアップを遮断して副記憶部３４０の内容を消去するようにしたので、プログラムやデータを暗号化されていない状態で扱う箇所をチップ内（システムＩＣ３００内）に限定することができ、かつシステムＩＣ３００外部の外部記憶部２００に記憶しておく時は暗号化することができる。暗号化されたデータは、復号化のための鍵がなければ解読することが非常に困難であるため現在の技術では外部からの攻撃に対して安全であると言える。

【００４９】すなわち、システムＩＣ３００内に暗号処理部３１０、監視部３２０、内部電源部３３０及び副記憶部３４０を組込み１チップ化されて構成されていることから、副記憶部３４０等を単独で取り出すことは極めて困難であることに加え、暗号化鍵／復号化鍵を記憶する副記憶部３４０は内部電源部３３０によりバックアップされ、監視部３２０が不正アクセスを検知すると瞬時に電源バックアップを遮断して副記憶部３４０の内容を消去するため外部からの不正使用は極めて困難である。

【００５０】上述したように、復号化のための鍵が強固に保護されていることから、仮に外部記憶部２００からプログラムやデータが読み出されたり、外部記憶部２００とシステムＩＣ３００間の信号線１５０上を通信する

プログラムやデータが読み取られることがあっても、暗号化されたデータを解読することは非常に困難である。

【００５１】以上のことからプログラムやデータの解析・改竄による不正な使用の脅威からシステムの安全を保持することができる。

【００５２】また、システムＩＣ３００内部に電源部を持つことにより、使用（通電）していないときでもシステムＩＣ３００単体での監視が可能である。また、内部電源が切れる時には、暗号化鍵を記憶している副記憶部３４０のデータを消去するようにしているので、暗号化鍵の漏洩を防ぐことができる。

【００５３】第２の実施形態

本発明の第２の実施形態に係るシステムＩＣは、基本構成は前記図１及び図２と同じであり、第１の実施形態とは副記憶部３４０のデータ消失方法が異なる。以下、第１の実施形態と異なる部分についてのみ説明する。

【００５４】本実施形態に係るシステムＩＣは、前記図１及び図２に示す監視部３２０が、システムＩＣ３００に対する外部からのアクセスを常に監視し、システムＩＣ３００に対して不正なアクセスがあった時、まず、副記憶部３４のデータを破壊するようにデータを書き換え、その後、内部電源部３３０に電源遮断指示を出して副記憶部３４０への電源供給を遮断させ、副記憶部３４の暗号化鍵／復号化鍵を消去する。

【００５５】例えば、暗号化鍵として、６４bitのＤＥＳを用いている場合、監視部３２０が不正アクセスを検知した時、副記憶部３４が記憶しているデータの任意のbit（わずか１bitでもよい）を書き換え、その後、副記憶部３４の暗号化鍵／復号化鍵を消去する。一般に、暗号化鍵において、１bitでもデータが書き換えられると全く異なる鍵となり殆ど完全にデータを破壊することができる。

【００５６】図４は本実施形態に係る監視手段３５０の監視部３２０の監視動作を示すフローチャートであり、前記図３に示すフローと同一ステップには同一符号を付して重複部分の説明を省略する。

【００５７】図４において、ステップＳＴ１で内部電源部３３０の出力電圧が所定値以下のとき、ステップＳＴ２で不正アクセスがあったとき、あるいはステップＳＴ３でセンサ入力に異常があったときは、システムＩＣに対して外部からプログラムやデータの解析・改竄のための不正使用が行われたと判断してステップＳＴ１１に進む。

【００５８】ステップＳＴ１１では、副記憶部３４のデータを破壊するように副記憶部３４が記憶しているデータの任意のbitを書き換えて強制的にデータを削除する。

【００５９】次いで、ステップＳＴ５で内部電源部３３０に電源遮断を指示し、内部電源部３３０から副記憶部３４０への電源供給を遮断する。これにより、副記憶部３４内の暗号化鍵／復号化鍵を消去する。

【００６０】以上説明したように、第２の実施形態に係るシステムＩＣは、監視部３２０が、システムＩＣに対する外部からのアクセスを常に監視し、システムＩＣに対して不正なアクセスがあった時、まず、副記憶部３４のデータを破壊するようにデータを書き換え、その後、内部電源部３３０に電源遮断指示を出して副記憶部３４０への電源供給を遮断させ、副記憶部３４の暗号化鍵／復号化鍵を消去するように構成したので、第１の実施形態で述べた効果をより一層高めシステムの安全を保持することができる。

【００６１】すなわち、第１の実施形態では、内部電源供給を遮断して、暗号化鍵を記憶している副記憶部３４０のデータを消去するようにしている。副記憶部３４０は、内部電源部３３０からの電源供給が絶たれると、極めて短い時間に記憶内容が消失する。しかし、最近では、メモリを低温保存すること等により電源供給が無くなったメモリからデータを読み取ることが可能になっている。また、内部電源部３３０からの電源供給を遮断して副記憶部３４０の記憶内容が失われる、極めて短い時間にデータを読み取ることも考えられる。

【００６２】そこで、第２の実施形態では、システムＩＣに対して不正なアクセスがあった時、副記憶部３４の記憶内容を破壊するようにデータを書き換え、データを強制的に削除することにより、上記暗号化鍵の漏洩の可能性を排除することができる。

【００６３】なお、第２の実施形態では、システムＩＣに対して不正なアクセスがあった時、副記憶部３４のデータを破壊するようにデータを書き換え、さらに、副記憶部３４０への電源供給を遮断させて、副記憶部３４の暗号化鍵／復号化鍵を消去するようにしているが、上記副記憶部３４の記憶内容の書き換えのみであってもよい。この場合は、内部電源部３３０の組み込みが必須ではなくなる効果を得ることができる。

【００６４】したがって、このような優れた特長を有するシステムＩＣを、電子マネーシステムの電子マネーの決済部に用いられるシステムＩＣに適用すれば、プログラムやデータの解析・改竄による不正な使用の脅威からシステムの安全性を格段に向上させることができる。

【００６５】なお、上記各実施形態に係るシステムＩＣを、上述したような電子マネーの決済部に適用することもできるが、勿論これには限定されず、演算処理部、主記憶部、通信制御を行う通信処理部を備え、外部記憶装置とアクセス可能な集積回路装置であれば全ての装置に適用可能であることは言うまでもない。

【００６６】また、上記各実施形態に係るシステムＩＣでは、信号線１５０を経由した外部記憶部２００間のアクセス例を示したが、外部記憶部２００には限定されず、外部装置の種類及び数、接続のインターフェースはどのようなものであってもよいことは勿論である。

【００６７】さらに、上記システムＩＣ、各部を構成する回路の種類、接続数、接続形態などは上述の実施形態に限られないことは言うまでもない。

【００６８】

【発明の効果】本発明に係る集積回路装置では、外部記憶装置からのプログラム及びデータを復号化するとともに、外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、内部電源部の電源供給により暗号化鍵／復号化鍵を保持する副記憶部と、集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると電源遮断指示する監視部と、副記憶部に電源を供給し、監視部から電源遮断指示があると副記憶部への電源供給を遮断する機能を有する内部電源部とを備えて構成したので、プログラムやデータの解析・改竄による不正な使用の脅威からシステムの安全を保持することができる。

【００６９】本発明に係る集積回路装置では、外部記憶装置からのプログラム及びデータを復号化するとともに、外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、暗号化鍵／復号化鍵を保持する副記憶部と、集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると副記憶部の記憶内容を書き換える監視部とを備えて構成したので、プログラムやデータの解析・改竄による不正な使用の脅威からシステムの安全を保持することができる。

【図面の簡単な説明】

【図１】本発明を適用した第１の実施形態に係る集積回路装置の構成を示すブロック図である。

【図２】上記集積回路装置の監視手段の構成を詳細に示すブロック図である。

【図３】上記集積回路装置の監視部の監視動作を示すフローチャートである。

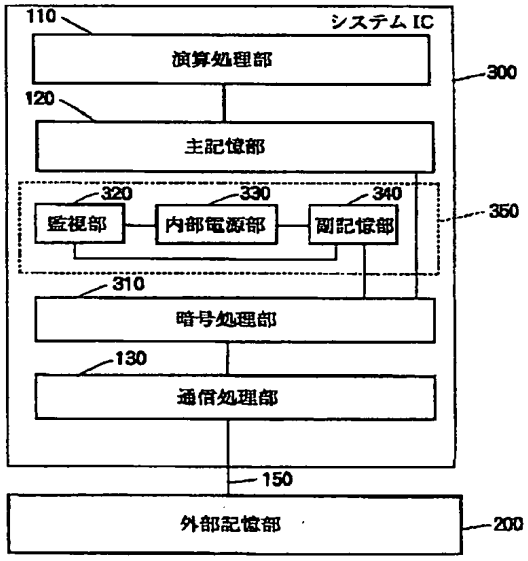
【図４】本発明を適用した第２の実施形態に係る集積回路装置の監視部の監視動作を示すフローチャートである。

【図５】従来の集積回路装置の構成を示すブロック図である。

【符号の説明】

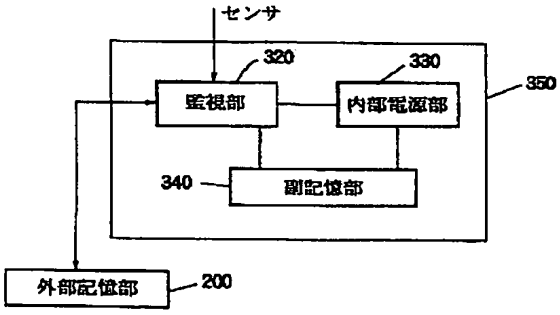
１１０　演算処理部、１２０　主記憶部、１３０　通信処理部、１５０　信号線、２００　外部記憶部（外部記憶装置）、３００　システムＩＣ（集積回路装置）、３１０　暗号処理部、３２０　監視部、３３０　内部電源部、３４０　副記憶部、３５０　監視手段

【図１】

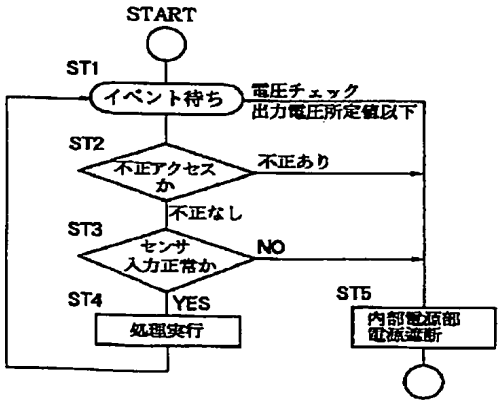


システムICの構成図

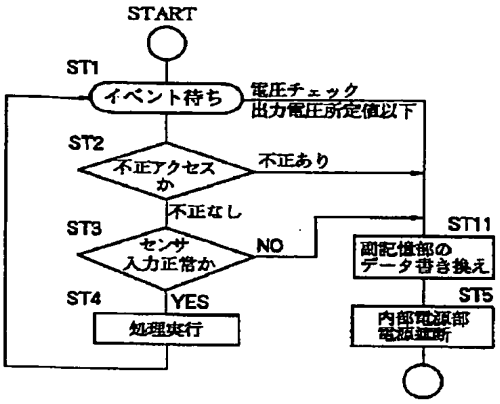
【図２】



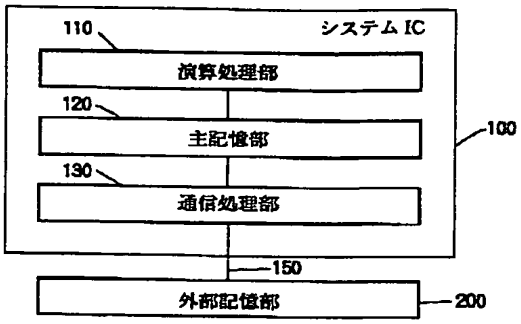
【図３】



【図４】



【図５】



従来のシステムICの構成図